Common Access Card Application

The introduction of smart cards and common access cards (CAC) can create real challenges in environments that require or prefer using KVM switch technology. Today, most KVM switches do not include support for any card readers.

Avocent has several solutions that support the use of smart cards and readers. This application brief will highlight these solutions and give instructions on how to implement these in several different environments.

Common Access Card Application

Table of Contents

3 Background Information about HSPD12
3 Desktop Applications
3 Data Center - Local Access Applications
3 Data Center - Remote Access Applications
3 Conclusion

Common Access Card Application

Background Information about HSPD12

Homeland Security Presidential Directive 12 (HSPD-12) was issued on August 12, 2007 and calls for a mandatory, government-wide standard for secure and reliable forms of ID, issued by the federal government to its employees and employees of federal contractors, for access to federally-controlled facilities and networks.

Today, many companies, in addition to government agencies, are using smart card or CAC to improve both physical security as well as the security of their network and the computers and servers attached to that network.

According to Gartner:

> "The creation of a system that relies on a single CAC as a means of validating identity for physical and logical security in an enterprise will, over time, enhance security, reduce card misuse and promote cost savings. Furthermore, when implemented correctly, this single CAC-type system can be used to promote a convergence between IT and physical security by promoting the blending of technology, people and processes for the overall defense of the enterprise. In addition, by 2011, 70% of enterprises implementing smart cards for network authentication will (also) follow a CAC approach."
>
> From March 3, 2008
> Gartner report "Using One Card for Access Control" ID Number G00155502

For a standard desktop user with one computer, the use of these smart cards is straightforward. After the computer is configured, the user inserts the smart card into an approved card reader to authenticate and use the computer.

For desktop environments with multiple computers or data center racks with multiple servers, smart card authentication can be much more complicated. This application brief will look at specific Avocent solutions that are designed to consolidate multiple computers at a desk or a rack and allow secure access using a single card reader.

Avocent develops a wide range of solutions to help manage IT equipment. Keyboard, video and mouse (KVM) switching is one widely deployed solution that allows multiple computers to be accessed from one or more set of peripherals. This is all done through physical consolidation of the KVM connections into a single piece of hardware.

Smart card/CAC support is primarily of interest to the government and large corporations that have significant regulatory requirements. The support is mainly a result of US government requirements, but also for any organization that is interested in allowing card access to desktop computers or servers. Avocent delivers support of smart cards/CAC in desktop and rack-based KVM switches to support applications that have multiple computers and those who want to use a CAC to authenticate and access them. Rack-based KVM over IP switches extend this capability by allowing a smart card reader to be mapped across a network in order to provide remote console access to servers using a smart card/CAC for authentication. All Avocent smart card/CAC enabled products support the USB smart card integrated Circuit(s) Cards Interface Device (CCID) specification.

What products does Avocent have to support this?

- For desktop environments with multiple computers, the SwitchView® SC switch family contains several models that support smart card/CAC readers. These models include 2-, 4- and 8-port switches which support VGA or DVI-I video. Certain models also support audio switching.
- In small and medium data centers that rely on local rack access, the AutoView® 2030 16-port analog KVM switch allows users to access all the attached servers in a rack using a single card reader. This switch includes an advanced on-screen display menu for easy management of the switch and fast server selection. The AutoView 2030 switch also includes a feature called virtual media that is not commonly found on most analog KVM switches. Virtual media allows a user to connect USB devices, including USB card readers, directly to the KVM switch and then map that connection out to any of the servers attached to the switch.
- For larger data center environments, where remote access is pervasive, a new technology is necessary to enable remote smart card authentication to the consoles of servers. In the data center, the Avocent DSView® 3 management software and KVM over IP switch appliances support smart card/CAC reader technology. This is critical in enforcing and tracking who has access to which IT systems and data and dictating who has control of data center management capabilities inside government systems and facilities.
  - The centralized management of DSView 3 software allows multiple Avocent appliances to be accessed and managed from a single browser interface. This makes deployment

and configuration changes to this equipment faster and also enables a detailed event log to track all system and user activity.

- The Avocent MergePoint Unity® KVM over IP and serial console switch supports local and remote virtual media and includes 4-, 8-, 16- and 32-port models. Remote virtual media enables users to virtually map USB devices across a network directly to the USB ports of a server attached to the KVM switch. This enables a user to virtually map a USB-based card reader and provide the user's credentials directly to the console of a server from anywhere. This remote out-of-band access is not dependent on the health of the operating system, the software applications or services running on the server or the network connectivity of the target device. The MergePoint Unity switches provide users the same access and capabilities of a local physical connection from anywhere. This technology allows smart card/CAC readers to be located away from the data center but still allows for secure connectivity to data center assets.

Desktop Applications

The first section will cover desktop environments where users have multiple computers and need to authenticate to each one using a CAC/smart card.

A basic, desktop KVM switch is a hardware device that allows users to control two or more computers with a single keyboard, video display and mouse. By pressing a button or a switch, users can easily access information and applications on completely separate systems. This boosts their productivity and saves space by eliminating the need to swap back and forth between multiple monitors and interface devices, saves cost of multiple peripherals, generates less heat in the user's area and saves power. Over the years, these desktop KVM switch products have improved to support higher video resolutions, audio, USB devices and enhanced security features.

Desktop KVM switching is particularly useful for security analysts who need to access information stored at different levels of classification on physically separate systems. Secure desktop KVM switches are specialized devices that include high-grade security features which assure the integrity of classified or sensitive data.

At the desktop, the Avocent SwitchView SC switch line is validated by the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Assurance Scheme (CCEVS) to EAL 4+ and incorporates additional security features to ensure data protection in the secure environment without limiting the user experience. These features ensure users, such as security analysts, can use just one console to safely access data stored on multiple computers– each operating at different levels of classification, saving time and reducing complexity.

Beyond their basic switching functions, secure KVM switches allow agencies to balance convenient access with their policies. They also help agencies reduce complexity and costs. For example, a secure desktop KVM switch may allow a single CAC reader to identify and authenticate users for up to eight connected computers. That saves agencies from purchasing a dedicated reader for every computer in use.

For desktop applications, the following SwitchView SC switch models support USB smart card/CAC readers.

DESKTOP KVM SWITCH	NUMBER OF PORTS	PLATFORMS SUPPORTED
SC220	2	USB and/or PS/2, VGA
SC240	4	USB and/or PS/2, VGA
SC280	8	USB and/or PS/2, VGA
SC420	2	USB, DVI-I, audio
SC440	4	USB, DVI-I, audio
SC540	4	USB, Dual Head DVI-I, audio

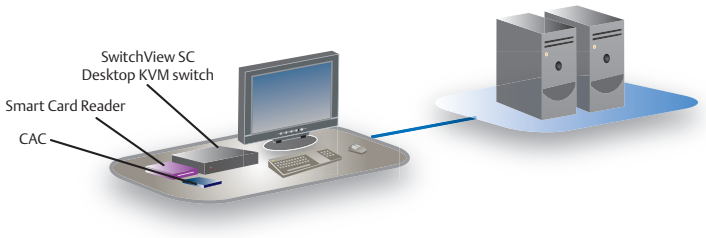


Figure 1: Desktop KVM switches with USB smart card/CAC reader support allow a user to share a single card reader across multiple computers. These KVM switches include models with 2, 4 or 8 ports and include options for VGA or DVI-I video and audio support.

Desktop KVM switching is particularly useful for security analysts who need to access information stored at different levels of classification on physically separate systems. Secure desktop KVM switches are specialized devices that include high-grade security features which assure the integrity of classified or sensitive data.

How does it all connect?
All of the computers will physically attach to the KVM switch using cables that provide keyboard, video and mouse and USB connectivity. These 6- and 12-foot cables are sold separately.

A single keyboard, video and mouse will connect to the desktop KVM switch user ports to allow access and control of all the attached computers. The USB smart card/CAC reader will attach directly to the KVM switch to allow the user to select an attached computer and authenticate using the smart card/CAC.

How will the card reader work?
Front panel push-buttons allow a user to switch KVM sessions and the card reader together. An amber LED indicates the target device to which the KVM session and card reader port are connected.

Data Center - Local Access Applications

This section will cover rack-based environments where users have multiple servers and need to consolidate local access to all the equipment and also authenticate using CAC/smart cards.

The AutoView 2030 KVM switch provides local support for your USB and/or PS/2 keyboards and mice and provides support for USB, PS/2, Sun® and serial target devices. The virtual media feature allows media such as CD-ROMs, flash memory and external drives to be virtually attached to a server's USB port. This virtual media feature also enables users to map USB-based smart card readers and open a virtual reader (VReader) session to the attached servers.

In environments that utilize CAC/smart cards, the switch allows each user to authenticate to the attached servers using a single, USB-based smart card reader. The OSCAR® graphical user interface (GUI) allows easy configuration of the switch and quick server selection.

For desktop applications, the following AutoView KVM switch supports locally attached USB devices including CAC/smart card readers.

RACK-BASED KVM SWITCH	NUMBER OF PORTS	PLATFORMS SUPPORTED
AutoView 2030	16	PS/2, USB, Sun and Serial

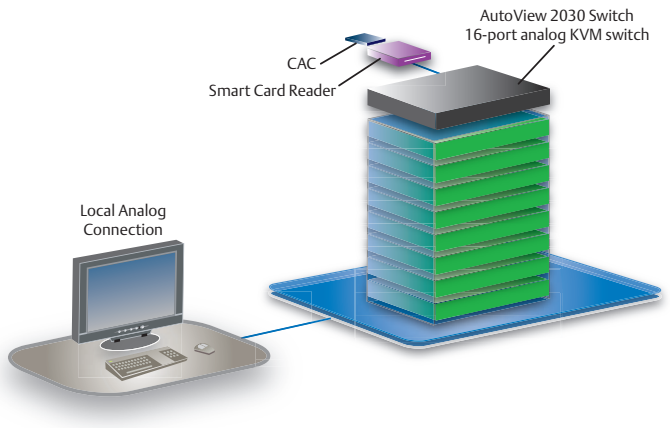


Figure 2: The 16-port AutoView 2030 KVM switch includes USB smart card reader support to allow a user to share a single card reader across multiple servers in a rack.

How does it all connect?
All of the computers will physically attach to the AutoView 2030 KVM switch using CAT-5 based adapters. These adapters provide keyboard, video, mouse and USB connectivity to the servers and allow for custom CAT-5 cable lengths up to 100 feet. For CAC/ smart card reader support, the AVRIQ-VMC module (sold separately) must be used.

The server interface module automatically assigns and retains unique server names for each attached server, which simplifies installation and eases reconfiguration

A single keyboard, video and mouse or LCD tray will attach locally to the AutoView 2030 switch to allow access and control of the attached servers. The USB smart card reader will attach directly to the KVM switch to allow any user accessing the rack the ability to select a server and authenticate using the smart card.

How will the card reader work?

The AutoView 2030 switch features compatibility with USB CCID-compliant smart card readers. To enable your smart card, plug your smart card into the front panel USB connector or one of User A's USB connectors on the rear panel of the switch and follow the steps below.

To connect your smart card:

1. Press **Print Screen** to launch the OSCAR interface on the AutoView 2030 switch.
2. Use the **Arrow** keys to highlight the server name which you wish to utilize your smart card, and then press **Enter**.

3. Press **Print Screen** to re-open the main dialog box.
4. Click *VReader*. The VReader dialog box displays.

5. Click to enable or disable the desired access options:
   - *Smart Card Reader* - Selects the detected smart card reader for VReader connections
   - *Auto Connect* - Sets the global setting for all VReader modules to auto connect for VReader connections
   - *Auto Disconnect* - Sets the global setting for all VReader modules to auto disconnect for VReader connections
6. Click *OK* to accept the options you have selected and return to the main dialog box.

NOTE: The AutoView 2030 switch detects smart card insertion and removal events and notifies the connected target when one of these events occurs. To open a virtual reader session (VReader) with a server, the server must first be connected to the switch using an AVRIQ-VMC module.

Data Center - Remote Access Applications

This section will cover rack-based environments where users have multiple servers and need to consolidate local and remote access to all the equipment and also authenticate using CAC/smart cards.

The Avocent MergePoint Unity switches include both KVM over IP and serial console management technology in a single appliance. This provides IT administrators a complete, remote management solution to access and control servers, networking equipment and other devices found in data centers and branch offices.

The MergePoint Unity switches enhance the in-band management typically done through the Network Interface Card (NIC) of IT equipment by providing secure and remote out-of-band connections directly to the physical KVM, USB and serial ports. This unified approach provides IT administrators a faster method to diagnose, reconfigure or restore equipment to meet SLAs and minimize downtime.

The Avocent DSView 3 management software provides centralized management of the entire IT infrastructure. DSView 3 software also increases security by keeping users out of the data center and ensures comprehensive authentication and logging for device access. This improves efficiencies, lowers costs and enables faster troubleshooting and reduced downtime.

For remote access applications, the following MergePoint Unity switches include virtual media to allow users to map USB devices, including CAC/smart card readers, to the attached servers regardless of location.

SWITCH	USERS	PORTS	PLATFORMS	MANAGEMENT INTERFACE
MPU1004	1 local, 1 digital	4	PS/2, SUN, USB serial	DSView 3 software or onboard Web interface
MPU1008 OR MPU1008DAC	1 local, 1 digital	8	PS/2, SUN, USB serial	DSView 3 software or onboard Web interface
MPU1016 or MPU1016DAC	1 local, 1 digital	16	PS/2, SUN, USB serial	DSView 3 software or onboard Web interface
MPU2016 or MPU2016DAC	1 local, 2 digital	16	PS/2, SUN, USB serial	DSView 3 software or onboard Web interface
MPU2032 or MPU2032DAC	1 local, 2 digital	32	PS/2, SUN, USB serial	DSView 3 software or onboard Web interface
MPU4032 or MPU4032DAC	1 local, 4 digital	32	PS/2, SUN, USB serial	DSView 3 software or onboard Web interface
MPU8032 or MPU8032DAC	1 local, 8 digital	32	PS/2, SUN, USB serial	DSView 3 software or onboard Web interface

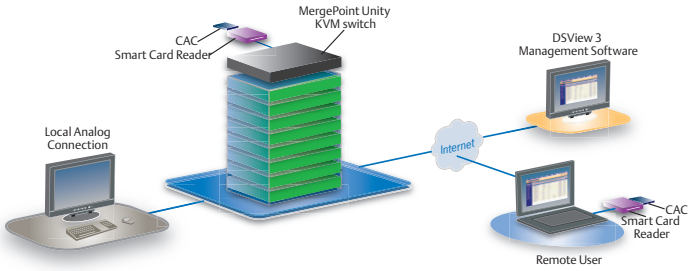


Figure 3: The MergePoint Unity appliance with USB smart card reader support allows local and remote users to map a USB-based card reader across multiple computers. These KVM switches include models with 4, 8, 16 and 32 ports and include options for 1, 2, 4 or 8 digital channels for one or more remote users to connect at the same time and select different servers. The DSView 3 software manages all the Avocent hardware and provides a single-browser interface to access all installed appliances.

How does it all connect?

All of the computers will physically attach to the MergePoint Unity appliance using CAT-5-based adapters. These adapters provide keyboard, video, mouse and USB connectivity to the servers and allow for CAT-5 cable lengths up to 100 feet. For CAC/smart card reader support the MPUIQ-VMC or DSRIQ-VMC module (sold separately) must be used.

The server interface module automatically assigns and retains unique server names for each attached server, which simplifies installation and eases reconfiguration.

A single keyboard, video and mouse or LCD tray will attach locally to the MergePoint Unity switch to allow local access and control of the attached servers. The USB smart card reader will also attach directly to the KVM switch to allow any user accessing the rack the ability to authenticate using a smart card when a server is selected.

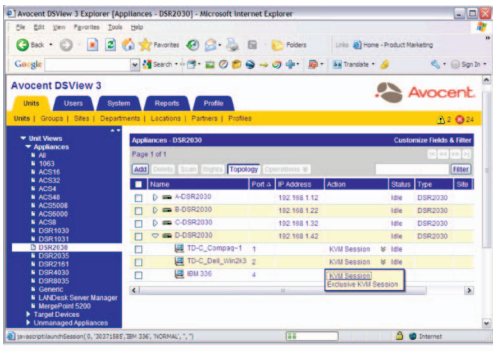
All the MergePoint Unity appliances support CAC/smart card readers in stand-alone applications using the built-in browser interface. In larger configurations, the DSView 3 software can provide consolidated management and access across multiple Avocent appliances.

The DSView 3 software can be installed as a virtual server or directly on a physical server and supports a wide range of operating systems. Multiple instances of the software may be installed to provide redundancy and multiple points of access for users in various locations or regions. The software will allow for granular permissions to be assigned so that individual users logging in will only see the servers that they have permission to access and control.

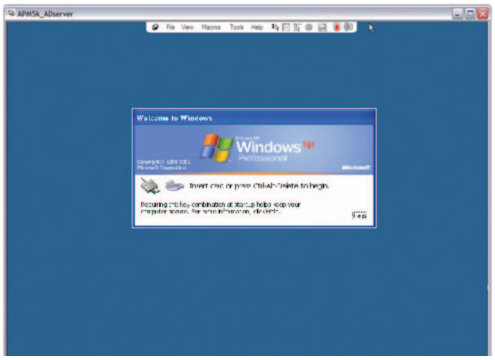
How will the card reader work?

To access a remote server and map a card reader:

1. Log in to the DSView 3 software and select a target to access. From the Action column select KVM Session to launch a remote connection.



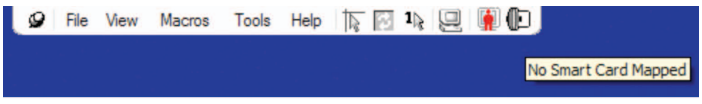
2. The Video Viewer window will open and display the connection to the selected server. Across the top of the session window is a toolbar that allows many functions, including the ability to map a USB-based card reader.



The smart card status is indicated by the smart card icon at the far right of the Video Viewer toolbar. The following table describes the smart card status icons.

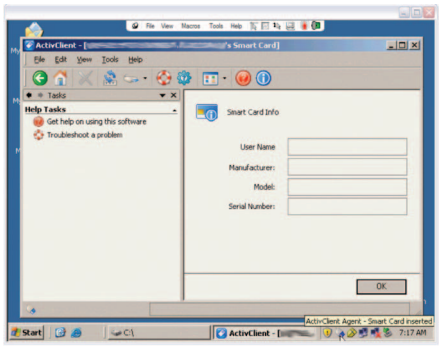
ICON	DESCRIPTION
	Disabled - A smart card reader is not available, the IQ module does not support smart card readers or smart card access is disabled in the DSView 3 software
	Not mapped - A smart card reader is available but has not been mapped yet
	Available - A smart card is mapped and available

At this point, the icon in the toolbar will show no smart card mapped.



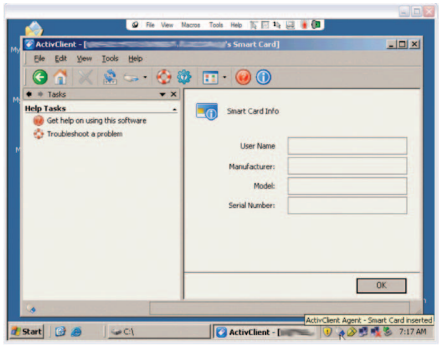
3. Insert a smart card into the smart card reader attached to your laptop/desktop client computer.

4. Click Tools - Map Smart Card on the Video Viewer window menu.



5. If no smart card is mapped to the target device, the No Card Mapped option will have a dot beside it. Select your smart card, listed below this option, to map the smart card.

6. Press Print Screen to re-open the main dialog box.



7. There are several options to close the remote session and unmap the smart card:

- Close out the KVM session by clicking X in the Video Viewer window menu.

-or-

- Select Tools - No Card Mapped.

-or-

- Remove the smart card from the smart card reader.

-or-

- Disconnect the smart card reader from the client server.

Video Viewer Session Properties

Session properties specify whether users may share Video Viewer sessions automatically and whether shared connections may be viewed with the Video Viewer View - Connected Users command.

To change Video Viewer session properties for use with smart cards:

You must have DSView 3 software administrator or user administrator privileges to configure Video Viewer session properties.

1. Click the *System* tab in the DSView 3 Explorer.
2. Click *Global Properties* in the top navigation bar.
3. Select *Video Sessions* to open the Video Viewer Session Properties window.
4. To specify if smart card connections can be used in Video Viewer sessions, enable or disable *Allow Smart Cards to be used in Video Viewer sessions.*
5. To specify if a single available smart card can be automatically mapped, enable or disable *Automatically map the Smart Card when a single card is present.*
6. Click *Save* and then click *Close.*

Conclusion

KVM switches are widely deployed on desktops and in data centers around the world. Check your current KVM equipment to verify if it supports smart card readers or not. As more companies begin to use smart card technology, older KVM switch technology will need to be replaced to support this.

Avocent has several solutions that support the use of smart cards and readers. If you need help determining the best product for your environment, please contact us or visit www.avocent.com.

About Emerson Network Power

Emerson Network Power, a business of Emerson (NYSE:EMR), is the global leader in enabling Business-Critical Continuity™ from grid to chip for telecommunication networks, data centers, health care and industrial facilities. Emerson Network Power provides innovative solutions and expertise in areas including AC and DC power and precision cooling systems, embedded computing and power, integrated racks and enclosures, power switching and controls, monitoring and connectivity. All solutions are supported globally by local Emerson Network Power service technicians. Aperture and Avocent solutions from Emerson Network Power simplify data center infrastructure management by maximizing computing capacity and lowering costs while enabling the data center to operate at peak performance. For more information, visit www.Aperture.com, www.Avocent.com or www.EmersonNetworkPower.com.

Emerson Network Power.
The global leader in enabling Business-Critical Continuity™.

EmersonNetworkPower.com

- AC Power
- Connectivity
- DC Power
- Embedded Computing
- Embedded Power
- Infrastructure Management & Monitoring
- Outside Plant
- Power Switching & Controls
- Precision Cooling
- Racks & Integrated Cabinets
- Services
- Surge Protection

Emerson, Business-Critical Continuity and Emerson Network Power are trademarks of Emerson Electric Co. or one of its affiliated companies. ©2010 Emerson Electric Co.
0810-CAC-AB-EN